Security Whitepaper

Overview:

Zoolz is a backup service that creates a continuous real time backup of your system and data providing your company with a scalable, reliable and a secure backup solution. Since data security is pivotal to the provider and user of backup software, Zoolz uses the highest security standards in transferring your data to and from our data centers. Using military-grade encryption, the user's data is protected from cyber attacks, unauthorized access, and theft. This white paper discusses in further detail the methods employed to protect your data.

Authorization:

This section discusses achieving security in the communication between Zoolz and the customer's system. With regards to communication, the following measures are used to ensure maximum security:

- Unlike other cloud backup solutions, Zoolz does not use a session-based connection which can prove a security risk since the session ID can enable unauthorized access to the data on a user's account from any source possessing the session ID. Instead, and for enhanced security, authenticating the user's credentials is done per request. The authentication process is explained in further detail below:

  Authentication is done using a hash function on the client that takes the user's password and timestamp as inputs generating a value that is sent along with the username to the server. Here the server compares this value with the value it calculates from the same inputs (password and timestamp) associated with the username stored on the server. If the results of the hash functions on both the client and server are identical, the user is authenticated and the request is processed.

- Communication is done using two Secure Sockets Layer (SSL) TCP connections through port 443.

- Both connections use two way SSL Certificate verification, trusted server certificates, as well as encryption key and client (EXE) certification.

- Communication with the cloud is <u>always</u> initiated by the user's agent.

Data Write (Backup):

Writing data to the cloud (backup) is a process designed to provide maximum security to the user's data. This section discusses the security features that ensure the process of writing data to the cloud (backup) is most secure.

Step 1:
The backup process starts by encrypting the data on the user's local machine.

The encryption algorithm used by Zoolz is the Advanced Encryption Standard (AES 256) algorithm which is the encryption standard for the US Government and the Department of Defense.

The user is given two options, either to provide their own personal code for encryption, and in this case they are the only party which possesses the code and can decrypt the data.

The second option is to use a unique auto-generated encryption key provided with their Zoolz software. In this case, the encryption key is also stored securely on our servers along with the user's private information.

The encryption is done on the fly as the data is read, and all files are encrypted to a temp folder, and each is securely deleted after it has been successfully uploaded or if the backup is canceled by the user.

Step 2:
A connection is established as data will be transferred securely to Zoolz Servers using SSL connections.

Data is subdivided into segments that are each encrypted and the authentication process is done each time a segment is sent to Zoolz Servers.

Step 3:

Zoolz utilizes Amazon S3 Server Side Encryption employs strong multi-factor encryption. Each object is encrypted with a unique key. As an additional safeguard, this key is itself encrypted with a regularly rotated master key. Amazon S3 Server Side Encryption uses one of the strongest block ciphers available -- 256-bit Advanced Encryption Standard (AES-256) -- to encrypt your data.

Data Read (Restore):

Zoolz offers several solutions for data restoration. The user can restore their data using the Client Agent on their system, the web interface, or even a mobile device such as an iPhone or an Android-based device. Meanwhile, data security is ensured and guaranteed regardless of the method used to restore data:

Authentication is required:

Whether the user is using the client agent on their system, the web interface, or a mobile device, security is ensured by authenticating the user's credentials every time a request is sent. The user has to provide their credentials (Email address, password, and encryption password if enabled) in order to access the backup database.

Method I: Restore using the Client Agent:

Just as the data is encrypted on the user's local system before being transferred to the cloud, **the data is always only decrypted on the user's system.** If the user chose a personal encryption password, they are prompted to enter the encryption password when attempting to restore data. A hashed **(SHA265)** version of the password is sent to be compared with the one on the cloud (the cloud only stores a hashed version of the password – the hashed version cannot be decoded to give the original password and cannot be used to decrypt the data). Once the encryption password is authenticated the data is sent to the user. Once the data is received it is decrypted using the encryption password provided by the user. In the case of the user choosing the auto-generated encryption key, the key is automatically fetched, hashed, and then sent to the servers for authentication.

Method II: Restore using a Mobile device:

Even when a mobile device is used to restore data, the decryption takes place on the device and not on the cloud. Zoolz mobile software was designed to be capable of performing decryption of data restored from the cloud.

Method III: Restore from Web:

- *In order to access the backup database on the website, users must log in using their Email address and password (see authentication).*

When the authentication process is successful, the user is prompted for the encryption password (in the case of personal encryption), requested data is fetched from storage while in encrypted form, then transferred to the user's agent and decrypted on the fly. **There is no decrypted copy saved on the server.**

Data Storage:

Zoolz is a pure-cloud solution. Multiple cloud storage providers are utilized to securely store the user's data. The list currently includes *Amazon S3 and Amazon Glacier*. This service provider is among the most trusted in the business as they provide the highest standards of data availability and service reliability.

Data in storage is always present in an encrypted form using the AES 256 Encryption Standard SSE.

Please refer to the following Whitepaper for detailed information on the security and features of the storage services utilized by Zoolz.

Conclusion:

This white paper described the principal security measures offered by Zoolz to ensure the safety of the user's data. A Secure deployment of the software, transfer security, data encryption, and storage security all prove Zoolz to be a safe and a reliable cloud backup solution designed and constructed with security in mind.